

IN THE U.S. PATENT AND TRADEMARK OFFICE



Applicant(s): INADA, Toru et al.

Application No.:

Group:

Filed: July 5, 2001

Examiner:

For: CRYPTOGRAPHIC APPARATUS AND CRYPTOGRAPHIC COMMUNICATION
SYSTEM

L E T T E R

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

July 5, 2001
0054-0236P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
JAPAN	2000-223961	07/25/00

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: 

JOHN CASTELLANO

Reg. No. 35,094

P. O. Box 747

Falls Church, Virginia 22040-0747

Attachment
(703) 205-8000
/kw

CERTIFIED COPY OF
PRIORITY DOCUMENT

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

INAHA, Ioru et al.
July 5, 2001
BSKB, LLP
1703) 205-8000
0054-0236 P
1 of 1

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2000年 7月25日

出願番号
Application Number:

特願2000-223961

出願人
Applicant(s):

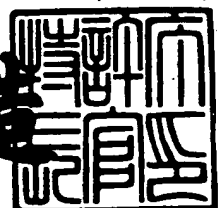
三菱電機株式会社



2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3013022

【書類名】 特許願

【整理番号】 525747JP01

【提出日】 平成12年 7月25日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/18

【発明者】

 【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会
社内

 【氏名】 稲田 徹

【発明者】

 【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会
社内

 【氏名】 後沢 忍

【特許出願人】

 【識別番号】 000006013

 【氏名又は名称】 三菱電機株式会社

【代理人】

 【識別番号】 100102439

 【弁理士】

 【氏名又は名称】 宮田 金雄

【選任した代理人】

 【識別番号】 100092462

 【弁理士】

 【氏名又は名称】 高瀬 彌平

【手数料の表示】

 【予納台帳番号】 011394

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号装置及び暗号通信システム

【特許請求の範囲】

【請求項 1】 端末間で送受信されるパケットデータを受信する平文パケット受信手段と、

前記パケットデータを暗号化した際のパケット長を計算し、前記パケット長と所定のパケット長とを比較して、前記パケットデータの分割が必要であるか否かを判定するフラグメント判定手段と、

前記判定の結果パケットデータの分割が必要であると判定された場合には、

前記パケットデータを複数の分割データに分割するとともに、送信先の端末装置において前記分割データを再組み立て可能な所定のデータ構造を有する複数の分割データパケットに、前記複数の分割データを夫々格納し、さらに当該夫々の分割データパケットに前記分割データ間の連続性を保証するための制御情報を付加するフラグメント処理手段と、

前記複数の分割データパケットを夫々別個に暗号化し複数の暗号化パケットを生成する暗号化手段と、

前記複数の暗号化パケットを送信先の端末に送信する暗号化パケット送信手段と、

を備えたことを特徴とする暗号装置。

【請求項 2】 端末間で送受信されるパケットデータを、送信側の暗号装置で暗号化し受信側の復号装置で復号化する暗号通信システムにおいて、

請求項 1 に記載の暗号装置と、

前記暗号装置から送信された複数の暗号化パケットを受信し、該複数の暗号化パケットを夫々別個に前記分割データパケットへと復号し、当該複数の分割データパケットを復号処理順に送信先の端末に送信する復号装置と、

前記複数の分割データパケットを受信し、各分割データパケットに付加された前記制御情報に基づいて分割データの再組み立てを行ってパケットデータを得る端末と、

を備えることを特徴とする暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを介して端末間で送受信されるパケットデータを暗号化する暗号装置及び暗号通信システムに関するものである。

【0002】

【従来の技術】

ネットワークに接続された複数の端末間で送受信するパケットデータを暗号化する方式で、「Security Architecture for the Internet Protocol」(IPSEC-RFC2401～2410、The Internet Society、1998)に代表されるエンカプセル暗号方式では、暗号化されたパケットデータの前後にエンカプセル暗号化されたデータフィールドであることを明示するエンカプセルヘッダ及びテイラを付加する。したがって、暗号化されたパケットは、暗号化される前の平文パケットと比較してパケット長が増大する。

【0003】

一方、ネットワークを介して送受信されるパケットは、最大のパケット長が規定されており、それがエンカプセル暗号化されているか否かに拘わらず、前記最大パケット長以下で送信されることが規定されている。したがって、暗号化される前の平文パケットのパケット長が前記最大パケット長以下であっても、エンカプセル暗号化の結果パケット長が増大し前記最大パケット長より長くなった場合には、該暗号化パケットをネットワークを介して送信する以前に前記所定のパケット長以下の複数のパケットに分割する必要がある。このようなパケットの分割処理を、以下では「フラグメント処理」と呼ぶ。

【0004】

一方、前記複数の分割パケットを受信した復号装置では、前記フラグメント処理によって分割された複数の分割パケットを一つのエンカプセル暗号化されたパケットに再組み立てした後に、該暗号化パケットを平文パケットに復号化する。復号装置における暗号化パケットの再組み立て処理を、以下では「リアセンブル

処理」と呼ぶ。

【0005】

前述のエンカプセル暗号方式においてパケットデータを復号化するには、復号時に前記フラグメント処理された複数の分割パケットの全てが復号装置に受信されている必要がある。しかし、一般に送信側の暗号装置と受信側の復号装置とを接続するネットワーク上では、パケットの送達に要する遅延時間がパケット毎に一定ではなく、パケットが送達される順序も保証されない。したがって、復号装置でパケットデータを復号化する際に、前記フラグメント処理された複数の分割パケットが全て受信されるのを待つ「待機時間」が生じる。

【0006】

これに対し、例えば特開平9-200195号公報に示された従来の暗号通信方式のように、予めフラグメント処理が生ずるか否か判定した上で、暗号化処理前にパケットを分割し、分割されたパケットをそれぞれエンカプセル暗号化して送信することにより、復号装置における分割パケット受信の待機時間を低減させる暗号方式が提案されている。

【0007】

以下で、前記従来の暗号通信方式におけるパケットデータの処理手順を図3の説明図に従って説明する。まず送信元の端末は、送信先端末に送付すべきデータである「IPデータ」20dと、送信元端末から送信先端末までのネットワーク上の経路の特定や複数の平文パケット間のIPデータの連続性の保証等に用いられる制御情報が収録された「IPヘッダ」20bとからなる「IPパケット」を作成し、これにデータの発信元及び送信先の端末を特定する物理アドレスが収録された「MACヘッダ」20aを付して送信する。前記端末間ではインターネット・プロトコル(IP)に従ってパケットデータの送受信が行なわれており、送信先の端末では前記IPパケットのデータ構造を有するパケットデータを受信することが可能である。なお、送信元の端末によって作成される未だ暗号化されていないデータパケット20を以下では「平文パケット」と呼ぶ。

【0008】

送信側の暗号装置は、前記平文パケット20を受信し暗号化処理を開始する。

ここで暗号化の対象となるのは、前記平文パケット 2 0 のうち I P パケットの部分、即ち I P ヘッダ 2 0 b 及び I P データ 2 0 d に含まれる情報である。

【 0 0 0 9 】

まず前記暗号装置は、受信された平文パケット 2 0 のパケット長と最大パケット長とを比較し、該平文パケット 2 0 のパケット長が前記最大パケット長よりも長い場合には、フラグメント処理を行って分割データ 4 1、4 2 を作成する。また暗号装置は、各分割データ 4 1、4 2 に、分割データ間の連続性を示す「分割識別子」を付加する。

【 0 0 1 0 】

次に暗号化装置は、前記分割データ 4 1 及び 4 2 を夫々別個に暗号化し、「暗号化データ」4 3、4 4 を得る。さらに暗号装置は、該暗号化データ 4 3、4 4 に、暗号化されたフィールドを明示する「E S P ヘッダ」4 5 c 及び「E S P テイラ」4 5 e、該暗号化データ 4 3、4 4 をネットワーク上に送信するための制御データが含まれた I P ヘッダ 4 5 b、送信先アドレスが記載された M A C ヘッダ 4 5 a を付加して暗号化パケット 4 5、4 6 を作成し、ネットワークを介して復号装置に送信する。なお前記暗号化の際、暗号化データに付加される前記 I P ヘッダ 4 5 b 及び E S P ヘッダ 4 5 c を、以下で「エンカプセルヘッダ」と呼ぶ。

【 0 0 1 1 】

前述の通り暗号化パケット 4 5、4 6 がネットワークを介して復号装置に受信されるまでの送達遅延時間は一定ではなく、復号装置への送達順序は保証されない。前記暗号化パケット 4 5、4 6 のうち、初めに暗号化パケット 4 6 を受信した復号装置は、前記エンカプセルヘッダ及び E S P テイラ 4 6 を検出してエンカプセル暗号化された暗号化データ 4 4 を抽出しこれを復号化して分割データ 4 2 を得る。

【 0 0 1 2 】

送信先の端末は、前述の通りインターネット・プロトコル（I P）に従いパケットデータを受信する。しかし前記復号化された分割データ 4 2 は、I P ヘッダを含んでいないので、I P ヘッダ及び I P データからなる I P パケットのデータ

構造を有さず、送信先の端末は、該分割データ 4 2 を受信することが出来ない。
したがって復号装置は、該分割データ 4 2 を送信先の端末に転送せずに一旦蓄積する。

【0013】

次に IP データの前半が格納された暗号化パケット 4 5 が受信されると、復号装置は暗号データ 4 3 の抽出、復号化を行って分割データ 4 1 を得る。全ての分割データ 4 2、4 1 が得られると、復号装置は、各分割データに夫々付されている分割識別子を拠所として分割データのリアセンブル処理を行い、暗号化対象となった IP ヘッダ 2 0 b 及び IP データ 2 0 d からなる IP パケットを得る。次に復号装置は、前記 IP パケットに送信先の端末を特定するアドレスを格納した MAC アドレス 4 7 a を付加して平文パケット 4 7 を作成し、該平文パケット 4 7 を所定の端末に送信する。

【0014】

ところで、パケットデータの送受信を行う端末は、連続して受信した複数の平文パケットに格納された IP データを夫々抽出するとともに、各平文パケットの IP ヘッダに含まれた IP データの連続性に関する制御情報を参照して、前記複数の IP データを結合して有意なアプリケーションデータを生成する「IP リアセンブル機能」を備えるのが一般的である。

【0015】

ここで前記従来の暗号通信方式において、前記復号装置における分割データのリアセンブル処理は、前記端末の IP リアセンブル機能とは別個独立に行なわれる。

【0016】

【発明が解決しようとする課題】

前記復号装置は、受信された暗号化パケット 4 5、4 6 を夫々別個に復号化して分割データ 4 1、4 2 を得る。しかし当該各分割データ 4 1、4 2 は、元の平文パケット 2 0 の IP ヘッダ 2 0 b 及び IP データ 2 0 d をフラグメント処理したものであり、フラグメント処理後の各分割データが有意な IP パケットとして夫々認識されるために必要な制御情報が収録された IP ヘッダが含まれておらず

、IPパケットのデータ構造を有さないため、送信先の端末に送信することは出来ない。したがって復号装置は、復号化された分割データ42、41を一旦蓄積し、全ての分割データが得られた後にリアセンブル処理を行って、送信先の端末が受信可能な、IPヘッダ20b及びIPデータ20bからなるIPパケットを作成する必要がある。

【0017】

しかし、前述の通りネットワークを介して送受されるパケットの送達遅延時間は一定でなく、復号装置で受信する複数の暗号化パケット45、46の送達順序は保証されないため、復号装置が最初の暗号化パケット45を受信してから平文パケット47を作成し送信するまでに待機時間が生じる。パケット伝送の際に復号装置で生じる待機時間は、ネットワークのパケット伝送性能を低下させるといった問題がある。

【0018】

本発明は、前記課題を解決するためになされたものであり、パケットデータの送受信を行う端末に一般的に備えられているアプリケーションデータのIPリアセンブル機能を活用することにより、復号装置における待機時間を削減させることが可能な、所定のデータ構造を有する暗号化パケットを生成する暗号装置と、該暗号装置を適用した暗号通信システムを提供するものである。

【0019】

【課題を解決するための手段】

前記の課題を解決し、目的を達成するために、本発明にかかる暗号装置においては、端末間で送受信されるパケットデータを受信する平文パケット受信手段と、前記パケットデータを暗号化した際のパケット長を計算し、前記パケット長と所定のパケット長とを比較して、前記パケットデータの分割が必要であるか否かを判定するフラグメント判定手段と、前記判定の結果パケットデータの分割が必要であると判定された場合には、前記パケットデータを複数の分割データに分割するとともに、送信先の端末装置において前記分割データを再組み立て可能な所定のデータ構造を有する複数の分割データパケットに、前記複数の分割データを夫々格納し、さらに当該夫々の分割データパケットに前記分割データ間の連続性

を保証するための制御情報を付加するフラグメント処理手段と、前記複数の分割データパケットを夫々別個に暗号化し複数の暗号化パケットを生成する暗号化手段と、前記複数の暗号化パケットを送信先の端末に送信する暗号化パケット送信手段と、を備えたことを特徴とする。

【 0 0 2 0 】

次の発明にかかる暗号通信システムにあっては、端末間で送受信されるパケットデータを、送信側の暗号装置で暗号化し受信側の復号装置で復号化する暗号通信システムにおいて、前記暗号装置と、前記暗号装置から送信された複数の暗号化パケットを受信し、該複数の暗号化パケットを夫々別個に前記分割データパケットへと復号し、当該複数の分割データパケットを復号処理順に送信先の端末に送信する復号装置と、前記複数の分割データパケットを受信し、各分割データパケットに付加された前記制御情報に基づいて分割データの再組み立てを行ってパケットデータを得る端末と、を備えることを特徴とする。

【 0 0 2 1 】

【発明の実施の形態】

実施の形態 1.

図 1 は、本実施の形態 1 にかかる暗号通信システムの構成を示した構成図である。図 1 において、13 は有意なアプリケーションデータを平文パケットに格納して送信する端末、1 は送信側端末 13 から前記平文パケットを受信して暗号化する暗号装置、8 はネットワークを介して受信した暗号化パケットを復号化して平文パケットを得る復号装置、14 は前記復号装置 8 から復号化された平文パケットを受信する端末である。

【 0 0 2 2 】

送信側端末 13 と暗号装置 1、並びに復号装置 8 と受信側端末 14 は、例えば企業内ネットワークのように、第三者に傍受される恐れが無い安全なネットワークで接続されており、該ネットワーク上では暗号化されていない平文パケットが送受信される。このようなネットワークを以下では「平文ネットワーク」と呼ぶ。

【 0 0 2 3 】

一方、前記平文ネットワーク相互間は、例えばインターネットのように、第三者によって通信データの傍受盗用の恐れがある広域ネットワークで接続されている。そこで本実施の形態 1 において、当該広域ネットワーク上でやり取りされるパケットデータは、前記暗号装置 1 及び復号装置 8 によって暗号化した上で送受信される。このようなネットワークを以下では「暗号ネットワーク」と呼ぶ。

【 0 0 2 4 】

ここで前記暗号装置 1 において、2 は前記送信側端末 1 3 から平文ネットワークを介して平文パケットを受信する平文パケット受信部、3 は該平文パケットをエンカプセル暗号化する際にフラグメント処理が必要か否か判定するフラグメント判定部、4 は前記フラグメント判定部の判定結果に従い前記平文パケットをフラグメント処理するフラグメント処理部である。

【 0 0 2 5 】

また、5 は前記フラグメント処理部 4 によってフラグメント処理されたデータを暗号化する暗号化部、6 は前記暗号化データをエンカプセル化して暗号パケットを作成するエンカプセル部、7 は前記暗号化パケットを暗号ネットワークを介して前記復号装置 8 に送信する暗号化パケット送信部である。

【 0 0 2 6 】

一方、前記復号装置 8 において、9 は暗号ネットワークを介して前記暗号化パケットを受信する暗号化パケット受信部、1 0 は前記暗号化パケットから暗号化データを抽出するデカプセル部、1 1 は前記抽出された暗号化データを平文パケットに復号する復号化部、1 2 は復号化された平文パケットを平文ネットワークを介して前記受信側端末 1 4 に送信する平文パケット送信部である。

【 0 0 2 7 】

本実施の形態 1 では、前記端末 1 3 及び 1 4 はインターネット・プロトコル (I P) に従って、有意なアプリケーションデータをパケットに格納してデータ通信を行う。一般にパケットによりデータ通信を行う端末は、アプリケーションデータの送信時に、送信対象となるアプリケーションデータを複数の I P データに分割し、夫々の I P データに I P データ間の連続性を保証する制御情報を収録した I P ヘッダを付加する「 I P フラグメント機能」と、 I P パケットの受信時に

、前記 I P データ間の連続性を保証するための制御情報に基づき、アプリケーションデータの再組み立てを行う「I P リアセンブル機能」を備える。本実施の形態 1 においても、前記端末 1 3、1 4 は I P フラグメント機能及び I P リアセンブル機能を備えるものとする。

【 0 0 2 8 】

以下、前記の通り構成される暗号通信システムの動作を図 2 に従って説明する。図 2 は、本実施の形態 1 の暗号通信システムにおけるパケットデータの処理手順を示した説明図である。

【 0 0 2 9 】

まず暗号装置 1 の平文パケット受信部 2 は、送信側端末 1 3 から平文パケット 2 0 を受信する。該平文パケット 2 0 には、I P データ 2 0 d、送信先の端末 1 4 の物理アドレスを格納した M A C ヘッダ 2 0 a、送信側端末 1 3 から送信先の端末 1 4 までの接続経路を特定するための制御情報や I P データ間の連続性保証のための制御情報が格納された I P ヘッダ 2 0 b が含まれている。

【 0 0 3 0 】

次に前記平文パケット 2 0 は、フラグメント判定部 3 に転送されフラグメント処理の要否が判定される。まずフラグメント判定部 3 は、エンカプセル暗号化によって前記平文パケット 2 0 にエンカプセルヘッダ及び E S P テイラが付加された場合のパケット長を算出する。次に、前記算出されたパケット長と予め規定されている最大パケット長とを比較し、規定の最大パケット長よりも長い場合には、暗号化前にフラグメント処理が必要であると判断する。例えば、暗号ネットワーク上に送信する最大パケット長が 1 5 0 0 バイト以内と規定されている場合に、前記フラグメント判定部 3 によって算出されたエンカプセルヘッダから E S P テイラまでの全データ長が 1 5 0 0 バイトより長い場合には、フラグメント判定部 3 はフラグメント処理が必要であると判定する。

【 0 0 3 1 】

そしてフラグメント処理が必要であると判定された場合には、前記フラグメント判定部 3 は I P データの分割数と分割された各データのデータ長を決定する。ここで各分割データのデータ長は、各分割データに前記エンカプセルヘッダ及び

E S P テイラが付加された際に、前記規定の最大パケット長を超えない長さに決定される。

【 0 0 3 2 】

次にフラグメント判定部 3 は、平文パケット 2 0 をフラグメント処理部 4 に転送し I P データのフラグメント処理を要求する。該要求を受けたフラグメント処理部 4 は、前記決定された I P データの分割数と各分割データのデータ長に従い I P データのフラグメント処理を行う。以下で、フラグメント処理部 4 による I P データのフラグメント処理について説明する。

【 0 0 3 3 】

まずフラグメント処理部 4 は、前記フラグメント判定部 3 によって決定された分割数及び各分割データのデータ長に従って、前記平文パケット 2 0 の I P データ 2 0 d を分割データ 2 1 d、2 2 d に分割する。

【 0 0 3 4 】

次にフラグメント処理部 4 は、送信先の端末 1 4 で前記分割データ 2 1 d、2 2 d のリアセンブル処理を可能とするために、前記端末 1 4 が直接受信可能なデータ構造を有する複数の分割データパケットを作成する。本実施の形態 1 において、前述の通り端末間ではインターネット・プロトコル (I P) に従ってデータ通信が行なわれており、前記送信先の端末 1 4 は I P パケットの受信が可能である。そこでフラグメント処理部 4 は、該 I P パケットのデータ構造を有する分割データパケット 2 1、2 2 を作成し、前記各分割データ 2 1 d、2 2 d を夫々格納する。

【 0 0 3 5 】

前記分割データパケット 2 1、2 2 には、前記分割データ 2 1 d、2 2 d の他に、該分割データパケットの伝送制御に関する情報が収録された I P ヘッダ 2 1 b、2 2 b が付加される。当該 I P ヘッダ 2 1 b、2 2 b に収録される制御情報は、前記平文パケット 2 0 の I P ヘッダ 2 0 b に収録されていた制御情報に基づいて作成されるが、さらにフラグメント処理部 4 によって前記分割データ 2 1 d、2 2 d の連続性を示す制御情報が追加される。

【 0 0 3 6 】

前記分割データの連続性を示す制御情報として、各分割データパケットのIPヘッダ21b、22bには、例えば、「当該分割データに継続する分割データがある旨を示すフラグ」と「分割データの順番を示す番号」とが収録され、さらに最後の分割データ22dのIPヘッダ22bには「最後の分割データであることを示すフラグ」が収録される。

【0037】

以上の通りフラグメント処理部4によるフラグメント処理の結果、各分割データパケット21、22は送信先の端末14が直接受信可能なIPパケットのデータ構造を有するとともに、各分割データパケットのIPヘッダ21b、22bには分割データの連続性を示す制御情報が収録される。従って、当該分割データパケット21、22を受信した端末14では、当該端末14が備える前述のIPリアセンブル機能を使用することにより、前記分割データパケット21、22から元の平文パケットのIPデータ20dを復元することが可能である。

【0038】

フラグメント処理部4によるフラグメント処理が完了すると、分割データパケット21、22は暗号化部5に送付される。暗号化部5は、分割データパケット21、22を夫々別個に暗号化し、暗号化データ23、24を生成する。次にエンカプセル部6は、前記暗号化データ23に暗号化データの領域を明示するESPヘッダ25c及びESPテイラ25eと、暗号ネットワークを介して暗号化データを送信するための制御情報を格納したIPヘッダ25bを付加し、暗号化パケット25を作成する。同様に前記暗号化データ24にESPヘッダ26c、ESPテイラ26e及びIPヘッダ26bを付加し、暗号化パケット26を作成する。

【0039】

次に暗号化パケット送信部7は、前記平文パケット20のMACヘッダ20aから送信先端末14の物理アドレスを読み出し、これに基づいて前記暗号化パケット25、26にMACヘッダ25a、26aを付加する。該MACヘッダが付加された暗号化パケット25、26は、暗号ネットワークを介して復号装置8に送信される。以上が、IPデータのフラグメント処理が必要であると判定された

場合の暗号装置 1 におけるパケットデータの処理手順である。

【 0 0 4 0 】

一方、フラグメント判定部 3 によって I P データのフラグメント処理が必要無いと判定された場合には、フラグメント判定部 3 は、受信された平文パケット 2 0 の I P ヘッダ 2 0 b 及び I P データ 2 0 d を暗号化対象データとして暗号化部 5 に直接送付する。暗号化部 5 は前記 I P ヘッダ 2 0 b 及び I P データ 2 0 d を暗号化し、次にエンカプセル部 6 は暗号化データに I P ヘッダ、E S P ヘッダ及び E S P テイラを付してエンカプセル化し暗号化パケットを作成する。次に暗号化パケット送信部 7 は、前記暗号化パケットを暗号ネットワークを介して復号装置 8 に送信する。この場合は、フラグメント処理部 4 による I P データのフラグメント処理は行なわれない。

【 0 0 4 1 】

次に復号装置 8 における処理手順について説明する。まず暗号化パケット受信部 9 は、前記フラグメント処理された暗号化パケット 2 5、2 6 を受信する。ここで、各暗号化パケット 2 5、2 6 が復号装置 8 に送達されるまでの伝送遅延時間は一定ではなく、暗号化パケットの送達順序は保証されない。以下では、暗号装置から送信された複数の暗号化パケットのうち、暗号化パケット 2 5 が最初に受信された場合について説明する。

【 0 0 4 2 】

暗号化パケット受信部 9 は、暗号化パケット 2 5 を受信すると直ちにデカプセル部 1 0 に転送する。次にデカプセル部 1 0 は、該暗号化パケット 2 5 の E S P ヘッダ 2 5 c 及び E S P テイラ 2 5 e を検出して暗号化データ 2 3 を抽出し復号化部 1 1 に送付する。

【 0 0 4 3 】

次に復号化部 1 1 は、前記暗号化データ 2 3 を復号化し I P ヘッダ 2 1 b 及び分割データ 2 1 d からなる分割データパケット 2 1 を得る。次に平文パケット送信部 1 1 は、暗号化パケット 2 5 から M A C ヘッダ 2 5 a を送信先の端末 1 4 の物理アドレスを読み出し、これに基づいて前記分割データパケット 2 1 に M A C ヘッダ 3 1 a を付加して平文パケット 3 1 を作成する。作成された平文パケット 3

1 は、該復号装置に蓄積されることなく、平文ネットワークを介して送信先の端末 1 4 宛てに直ちに送信される。

【 0 0 4 4 】

次に暗号ネットワークを介して暗号化パケット 2 6 を受信すると、復号装置 8 は、前記と同様に暗号化データ 2 2 の抽出、復号化、平文パケット 3 2 の作成を行い、該平文パケット 3 2 を送信先の端末 1 4 宛てに送信する。

【 0 0 4 5 】

復号装置 8 から平文ネットワークを介して平文パケット 3 1 及び 3 2 を受信した端末 1 4 は、各平文パケットの I P ヘッダ 2 1 b、2 2 b から分割データ 2 1 d、2 2 d のデータの連続性を保証するための制御情報を読み出す。最後に端末 1 4 は、当該制御情報に基づき、アプリケーションデータの I P リアセンブル機能を用いて各平文パケットの分割データ 2 1 d、2 2 d を結合し、送信元の端末 1 3 で作成された I P データ 2 0 d を得る。

【 0 0 4 6 】

このような構成とすることにより、本実施の形態 1 の暗号通信システムにおいて、暗号装置 1 は、平文パケット 2 0 の I P データ 2 0 d を分割し、送信先の端末 1 4 でパケットデータの再組み立てが可能な I P パケットのデータ構造を有する複数の分割パケットデータ 2 1、2 2 を作成し、これらを夫々別個にエンカプセル暗号化して送信する。一方、受信側の復号装置 8 では各暗号化パケットの復号化のみを行い、分割データ 2 1 d、2 2 d の再組み立ては、受信側端末 1 4 が備える I P リアセンブル機能を使用して行う。従って、復号装置 8 で分割データ 2 1 d、2 2 d のリアセンブル処理を行う必要がないため、フラグメント処理された全ての暗号化パケットを受信し、分割データをリアセンブル処理ために必要であった待機時間が不要となり、暗号ネットワークのパケット伝送性能を向上させることができる。

【 0 0 4 7 】

なお、本実施の形態 1 の暗号通信システムにおいて、端末間ではインターネット・プロトコル (I P) に従いデータ通信が行なわれていたが、端末間のデータ通信に適用される伝送制御手順は I P に限定されるものではなく、パケット方式

の伝送制御手順であって、データ通信を行う各端末がパケットデータの分割及び再組み立ての機能を標準的に具備している伝送制御手順であれば、他の伝送制御手順であっても本発明の効果を得ることは当然に可能である。この場合、暗号装置 1 によって作成される分割データパケット 2 1、2 2 のデータ構造は、前記 I P パケットのデータ構造に代えて、前記伝送制御手順で規定されたデータ構造とされる。

【 0 0 4 8 】

また本実施の形態 1 の暗号装置 1 において、フラグメント判定部 3 は、平文パケット 2 0 のパケット長と予め規定された最大パケット長とを比較してフラグメント処理の可否を判定したが、フラグメント処理可否の判定の基準となるパケット長は最大パケット長に限定されるものではなく、この他にフラグメント処理可否の判定規準となるべき所定のパケット長が設定されている場合には、前記平文パケット 2 0 のパケット長を該所定のパケット長と比較してフラグメント処理の可否を判定する構成であってもよい。

【 0 0 4 9 】

【発明の効果】

以上のように、本発明によれば、暗号装置はパケットデータを分割し、送信先の端末で該パケットデータが再組み立て可能な所定のデータ構造を有する、複数の分割パケットデータを作成し、これらを夫々別個に暗号化して送信する。また復号装置は各暗号化パケットの復号化のみ行い、前記パケットデータの再組み立ては送信先の端末によって行なわれる。従って、前記復号装置においてパケットデータの再組み立てを行う必要が無いため、前記複数の分割パケットデータの受信待ちに要する待機時間が削減され、ネットワーク上の暗号化パケットの伝送性能を向上させることができる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態 1 の暗号通信システムの構成を示した構成図である。

【図 2】 本発明の実施の形態 1 の暗号通信システムにおけるパケットデータの処理手順を示した説明図である。

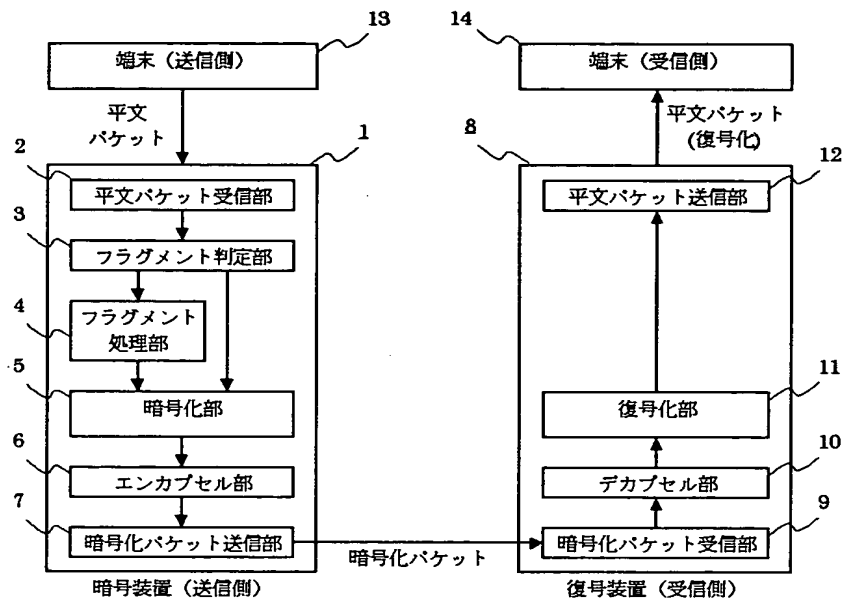
【図 3】 従来の暗号通信方式におけるパケットデータの処理手順を示した説明図である。

【符号の説明】

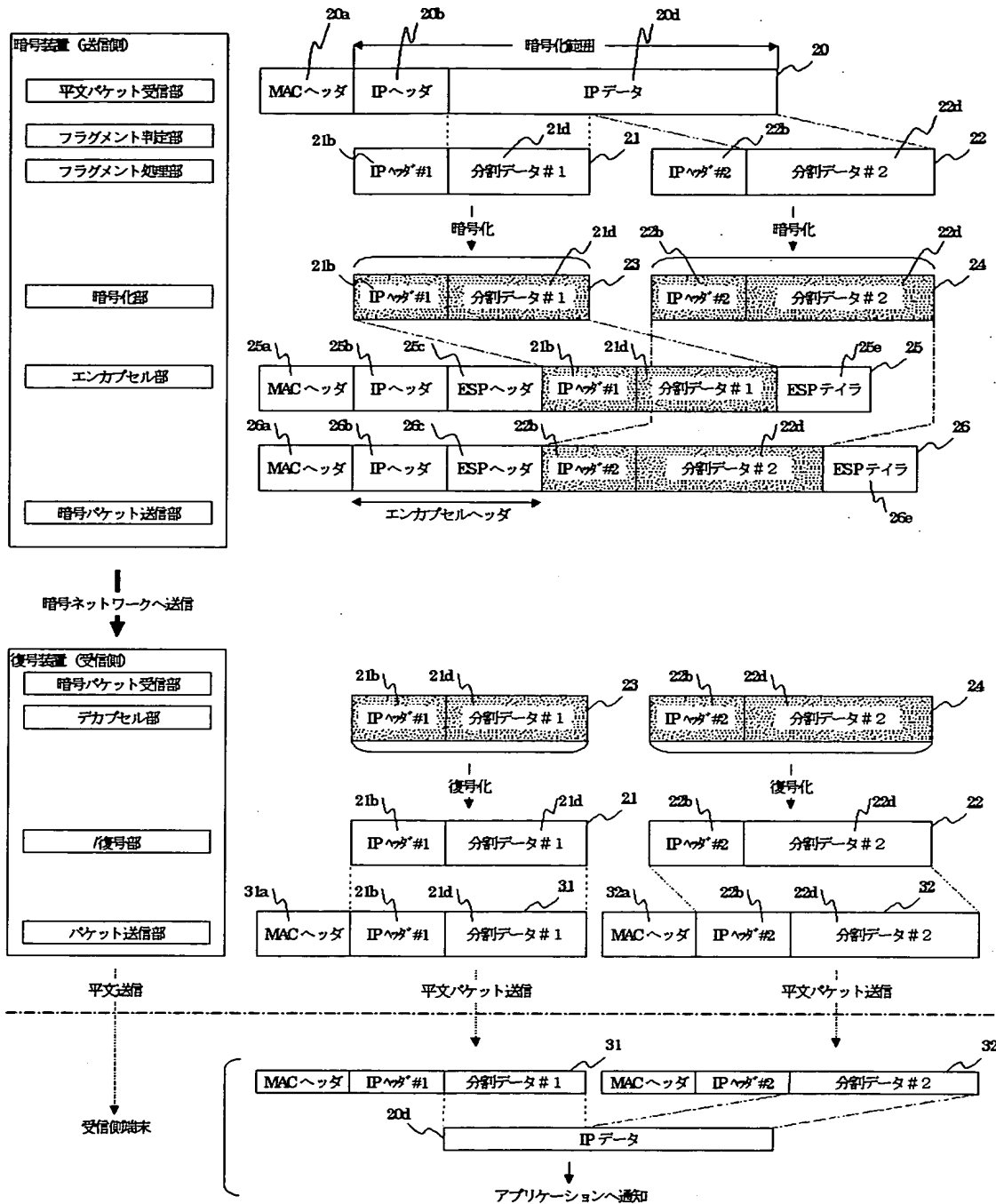
- 1 暗号装置
- 2 平文パケット受信部
- 3 フラグメント判定部
- 4 フラグメント処理部
- 5 暗号化部
- 6 エンカプセル部
- 7 暗号化パケット送信部
- 8 復号装置
- 9 暗号化パケット受信部
- 10 デカプセル部
- 11 復号化部
- 12 平文パケット送信部
- 13、14 端末
- 20、31、32、47 平文パケット
- 20a、25a、26a、31a、32a、45a、47a MACヘッダ
- 20b、21b、22b、25b、26b、45b IPヘッダ
- 20d IPデータ
- 21、22、45、46 分割データパケット
- 21d、22d、41、42 分割データ
- 23、24、43、44 暗号化データ
- 25、26 暗号化パケット
- 25c、26c、45c ESPヘッダ
- 25e、26e、45e ESPテイラ

【書類名】 図面

【図 1】

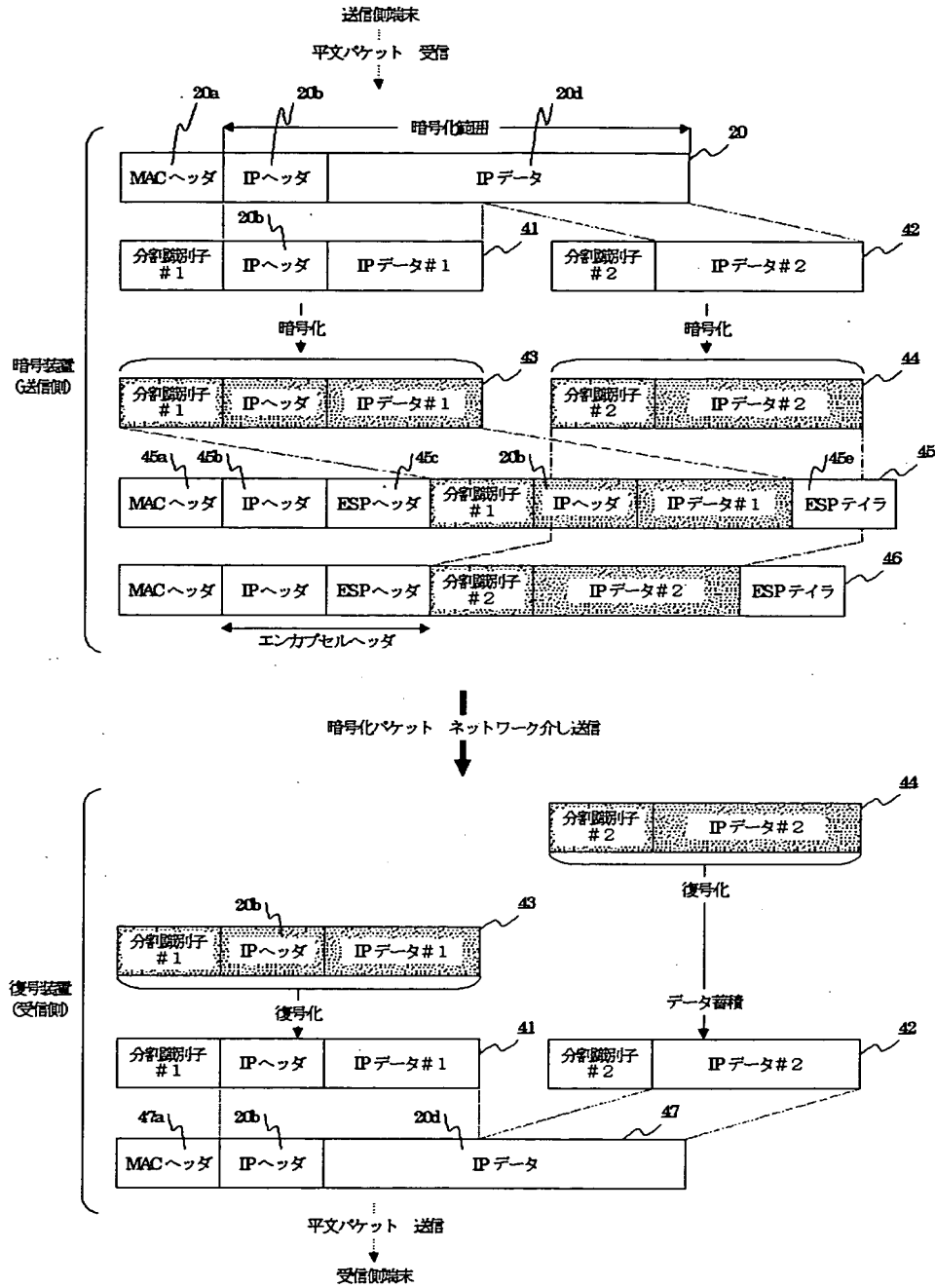


【図2】



20、31、32 平文パケット 21、22 分割データパケット
23、24 暗号化データ 25、26 暗号化パケット

【図 3】



20、47 平文パケット 41、42 分割データ
43、44 暗号化データ 45、46 暗号化パケット

【書類名】 要約書

【要約】

【課題】 端末間のパケットデータを暗号化する暗号通信システムで、復号装置における待機時間を削減させることが可能な暗号通信システムを得る。

【解決手段】 端末間で送受信されるパケットデータを送信側の暗号装置で暗号化し受信側の復号装置で復号化する暗号通信システムにおいて、前記暗号装置は、前記パケットデータの分割が必要であるか判定するフラグメント判定手段と、分割が必要であると判定された場合に複数の分割データに分割し、送信先の端末装置において前記分割データを再組み立て可能な所定のデータ構造を有する複数の分割データパケットに前記複数の分割データを夫々格納し、さらに当該夫々の分割データパケットに前記分割データ間の連続性を保証するための制御情報を付加するフラグメント処理手段と、前記複数の分割データパケットを夫々別個に暗号化する暗号化手段と、を備えたことを特徴とする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日 1990年 8月24日
[変更理由] 新規登録
住 所 東京都千代田区丸の内2丁目2番3号
氏 名 三菱電機株式会社